Proposal COM(2021) 206 of 21 April 2021 for a **Regulation** of the European Parliament and of the Council **laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)** and amending certain Union legislative acts.

EUROPEAN ARTIFICIAL INTELLIGENCE ACT

cep**PolicyBrief** 27/2021

Content

A. Essential contents of the proposed regulation

1 Objectives and Scope

- The Regulation contains EU-wide rules on the development, marketing and use of artificial intelligence ("AI"). This is intended to [Recitals 1 and 5]
  - strengthen the internal market,
  - protect health, safety and fundamental rights.

Authors: Dr. Lukas Harta, LL.M. und Dr. Matthias Kullas | kullas@cep.eu
cep | Kaiser-Joseph-Straße 266 | 79098 Freiburg | Germany | Telephone +49 761 38693-0 | www.cep.eu

- An AI system is a software
  - which can generate outputs – such as content, predictions, recommendations or decisions – for human-defined objectives and thereby influences their environment, and
  - is developed with one or more of the following techniques and approaches [Art. 3 (1), Annex I]:
    - machine learning approaches;
    - logic- and knowledge-based approaches, e.g. knowledge representation, inductive programming or inference and deductive engines;
    - statistical approaches, Bayesian estimation, search and optimisation methods.
- The Commission can adopt delegated acts to adapt the list of techniques and approaches to market trends and technological developments [Art. 4].
- The provisions of the Regulation apply to [Art. 2(1)]
  - providers of AI systems, from the EU and third countries, who place AI systems on the market or put them into service in the EU,
  - commercial and public-sector users ("users") of AI systems located within the EU and
  - providers and users located in a third country, where the output produced by AI systems is used in the EU.
- The Regulation takes a risk-based approach: particularly dangerous AI systems are prohibited whilst other AI systems are subject either to obligations according to the level of risk, voluntary codes of conduct or no AI-specific obligations.

2 Prohibited AI systems

- The following AI systems cannot be placed on the market, put into service or used:
  - AI systems which deploy "subliminal" techniques beyond a person's consciousness in order to influence their behaviour in a manner that may cause that person or another person "physical or psychological harm" [Art. 5 (1) (a)];
  - AI systems that exploit a vulnerability of a person due to their age or a physical or mental disability, in order to distort their behaviour in a manner that may cause that person or another person physical or psychological harm [Art. 5 (1) (b)].
- Public authorities are not permitted to place on the market, put into service or use AI systems which evaluate the trustworthiness of natural persons based on their social behaviour or personal characteristics ("social scoring") if this evaluation may be detrimental to certain persons [Art. 5 (1) (c)], namely
  - in social contexts which are unrelated to the contexts in which the data was originally generated or collected, or
  - in a manner that is unjustified or disproportionate considering the person's social behaviour or its gravity.

3 Real-time remote biometric identification systems

- A real-time remote biometric identification system is an AI system that can identify persons at a distance without a significant delay using biometric data without the user of the AI system having prior knowledge of whether the person will be present in the AI system's application area, e.g. real-time identification of persons in public places under video surveillance [Art. 3 (33) (36) and (37)].
- The use of real-time remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement – other purposes are governed by the General Data Protection Regulation (GDPR) – is only permitted when it is strictly necessary for [Art. (5) (1) (d)]
  - the targeted search for specific potential victims of crime or missing children,
  - the prevention of a specific, substantial and imminent threat to the life or physical safety of natural persons or of a terrorist attack, or
  - the detection, localisation, identification or prosecution of a perpetrator or suspect of a criminal offence if
    - a European arrest warrant can be issued for the offence irrespective of the criminal nature of the offence in the executing Member State – e.g. cases of rape, drug trafficking and counterfeiting – and
    - the maximum custodial sentence for the offence in the Member State deploying the real-time remote biometric identification system is at least three years.
  - The use of real-time remote biometric identification systems must be
    - provided for under national law [Art. 5 (4)] and

- authorised by a judicial authority or by an independent administrative authority, which may also take place retroactively in urgent cases [Art. 5 (3)].

4 High-risk AI systems

4.1 Definition

- An AI system is considered to be high-risk where it
  - is a product, or the safety component of a product, which is covered by existing EU health and safety harmonisation legislation and under these rules is subject to a conformity assessment by third parties, e.g. medical products, lifts and toys [Art. 6 (1), Annex II], or
  - is used in one of the following areas [Art. 6 (2), Annex III]:
    - biometric identification and categorisation of persons: the field of application is remote biometric identification;
    - management and operation of critical infrastructure: the field of application is use as safety components in road traffic and the supply of water, gas, heating and electricity;
    - education: the field of application includes determining access or assignment of persons to educational institutions and assessing students and participants in admission tests;
    - employment, workers management and access to self-employment: the field of application includes evaluating candidates in interviews;
    - access to and enjoyment of essential private services and public services and benefits: the field of application includes the evaluation of creditworthiness;
    - law enforcement: the field of application includes the assessment of whether a person will reoffend;
    - migration, asylum and border control management: the field of application includes the verification of the authenticity of documents;
    - administration of justice and democratic processes: the field of application is assisting a judicial authority in researching and interpreting facts and the law and in applying the law.
- By way of delegated acts, the Commission can add new fields of application within the listed areas if they represent a risk to health, safety or fundamental rights that, in terms of severity and probability of harm, is equivalent to the risks in the fields already listed. In this regard, the Commission takes particular account of the purpose of the AI system, the potential harm and the dependence of users on AI systems and their vulnerability [Art. 7(1) and (2)].

4.2 Requirements for high-risk AI systems

- Providers must ensure that high-risk AI systems meet the following requirements: They must
  - be developed using representative, error-free and complete data sets [Art. 10 (1), (3)];
  - be sufficiently transparent to enable users to interpret and use the results of the high-risk AI appropriately [Art. 13 (1);
  - be, in the light of their intended purpose, sufficiently accurate, robust and cybersecure [Art. 15 (1)];
  - automatically record events while operating [Art. 12 (1)] and
  - be designed for effective oversight by persons such that the latter can monitor the operation of the high-risk AI system and stop it as well as override its results [Art. 14 (1), (4)].

4.3 Obligations for providers of high-risk AI systems

4.3.1 Conformity assessment and due diligence obligations

- Prior to placing high-risk AI systems on the market, a conformity assessment must be carried out [Art. 16 (a) and Art. 19 (1)].
  - In the case of an AI system for remote biometric identification, the provider may carry out the conformity assessment [Art. 43 (1)]
    - with the involvement of a “notified body” or
    - itself, provided that the AI system is in conformity with a harmonised standard published in the Official Journal of the EU.
  - In the case of an AI system that is a product, or the safety component of a product, covered by existing EU health and safety harmonisation legislation and under these rules is subject to a conformity assessment by third parties, the conformity assessment is carried out by these third parties [Art. 43 (3)].
  - For all other AI systems, the conformity assessment is carried out by the provider itself [Art. 43 (2)].

– If an AI system is in conformity with a harmonised standard published in the Official Journal of the EU, conformity with the requirements for high-risk AI systems is presumed [Art. 40].

- Prior to placing a high-risk AI system on the market, providers must establish a risk management system which identifies the risks throughout its entire life-cycle [Art. 9 (1)].
  – Risk identification takes place by way of tests and a post-market monitoring system [Art. 9 (4) and Art. 61 (1), (2)].
  – Where applicable, risk management measures must be taken to ensure that the risk of the system is "acceptable" [Art. 9 (4)].
- Providers must draw up technical documentation and keep it up to date in order to demonstrate that their systems comply with the requirements for high-risk AI systems [Art. 11 (1) and Art. 18].
- Providers must provide instructions for use which include information on the characteristics, capabilities and limitations of the performance of their systems [Art. 13 (2), (3)].
- Providers must set up a quality management system that ensures compliance with the AI Regulation [Art. 17 (1)].

4.3.2 Reporting obligations

- Providers must report serious incidents and malfunctions to the surveillance authorities [Art. 3 (44) and Art. 62 (1)].
  – Serious incidents are any incident which may result in:
  - the death of a person or serious damage to a person's health,
  - serious damage to property or the environment or
  - serious and irreversible disruption of critical infrastructure.
  – Malfunctions are incidents that constitute a breach of EU law intended to protect fundamental rights.

5 Non-risk-based transparency obligations

- In the case of AI systems that are intended to interact with natural persons, providers must ensure that persons are informed of the fact that they are interacting with an AI system, unless this is obvious [Art. 52 (1)].
- In the case of AI systems for emotion recognition or biometric categorisation – these are systems which categorise persons e.g. according to age, gender, ethnic origin, sexual or political orientation – users must inform persons exposed thereto of the operation of the system [Art. 52 (2)].
- Users of "deep fake" AI systems, which manipulate image, audio or video content to resemble existing persons, objects or places and falsely appear to be authentic, must disclose that the content has been artificially generated or manipulated [Art. 52 (3)].

6 Codes of conduct

- The Commission and Member States shall encourage and facilitate the drawing up of codes of conduct by providers of AI systems and/or organisations representing them; the codes are intended to ensure [Art. 69]
  – that the requirements for high-risk AI systems are also applied to other AI systems or
  – that providers of AI systems voluntarily meet requirements that go beyond those in the Regulation, e.g. for sustainability or inclusivity.

7 Enforcement and monitoring

- Member States shall designate an independent monitoring authority ("market surveillance authority") to monitor the AI systems pursuant to the Market Surveillance Regulation [(EU) 2019/1020] [Art. 3 (26) and Art. 59 (2)].
  – The market surveillance authorities monitor whether AI systems and their use comply with the requirements of the Regulation.
  – The market surveillance authorities will be granted unrestricted access – including remote access –
  - to the training, validation and testing datasets used by providers [Art. 64 (1)] and
  - upon a reasoned request, to the source codes [Art. 64 (2)].
- If an AI system complies with this Regulation but presents a risk to the health or safety of persons, or to other aspects of public interest protection nevertheless, the market surveillance authority shall require the AI-

system provider, or other relevant operator, to take all appropriate measures to eliminate the risk, withdraw the AI system from the market or recall it [Art. 67 (1)].

- The market surveillance authority will report to the Commission on a regular basis the outcomes of its market surveillance activities [Art. 63 (2)].
- A "European Artificial Intelligence Board" - made up of the national market surveillance authorities and the European Data Protection Supervisor [Art. 57 (1)) – is established. It shall assist the Commission and the national market surveillance authorities, in particular, to [Art. 56]:
  - cooperate with each other,
  - ensure the consistent application of the Regulation in the EU and
  - analyse emerging issues in the Regulation's area of application.
- The Commission chairs the Board, convenes its meetings and prepares the agenda [Art. 57 (3)].

8 Sanctions

- Fines of up to € 30 million or 6 % of total worldwide annual turnover – for EU institutions, agencies and other bodies up to € 500,000 – may be imposed [Art. 71 (3), Art. 72 (2)]
  - for using prohibited AI systems,
  - for the unlawful use of real-time remote biometric identification systems and
  - for using a high-risk AI system developed with data sets which do not comply with the requirements of the Regulation.
- Fines of up to € 10 million or up to 2 % of total worldwide annual turnover may be imposed for supplying incorrect, incomplete or misleading information to notified bodies or national competent authorities [Art. 71 (5)].
- Fines of up to € 20 million or 4 % of total worldwide annual turnover – for EU institutions, agencies and other bodies up to € 250,000 – may be imposed for other breaches of the Regulation [Art. 71 (4), Art. 72 (3)].

B. Legal and political context

1 Legislative Procedure

21 April 2021	Adoption by the Commission
22 September 2021	Opinion European Economic and Social Committee
Open	Adoption by the European Parliament and the Council, publication in the Official Journal of the European Union, entry into force

2 Options for Influencing the Political Process

Directorates General:	DG Communications Networks, Content & Technology
Committees of the European Parliament:	Internal Market and Civil Liberties, Rapporteur Internal Market: Brando Benifei (S&D Group, IT); Rapporteur Civil Liberties: Dragoș Tudorache (Renew, RO)
Federal Germany Ministries:	Economy (leading)
Committees of the German Bundestag:	Economy (leading)
Decision-making mode in the Council:	Qualified majority (acceptance by 55% of Member States which make up 65% of the EU population)

3 Formalities

Competence:	Art. 16 TFEU (Data Protection), Art. 114 TFEU (Internal Market)
Type of Legislative Competence:	Shared competence (Art. 4 (2) TFEU)
Procedure:	Art. 294 TFEU (ordinary legislative procedure)

C. Assessment

1 Economic Impact Assessment

The Regulation constitutes regulatory discrimination against AI systems as compared with other technologies, particularly already established technologies. Legislation should however be technology-neutral. Rather than regulating AI systems, the Commission should focus its legislative provisions on achieving the desired regulatory goals. Thus, it is unclear why social scoring should only be prohibited when an AI system is used. What should rather be prohibited are machine-made decisions which have significant impact on the rights of a person or company, if such decisions cannot be corrected by a person, e.g. because the decision-making logic could not checked by a person due to its complexity (cf. cep**PolicyBrief** 4/2020).
The definition of AI systems used in the Regulation is too broad: it covers numerous software applications that have been used for years and are not "intelligent" but logic-based. Instead, the definition should take account of whether a system learns and makes decisions autonomously.
The Regulation creates a level playing field between EU and non-EU providers because it also applies to providers of AI systems that are not based in the EU. This also means that the provisions of the Regulation cannot be circumvented by deploying AI systems in third countries and using the results subsequently in the EU.
Clarification is required as to the meaning of "subliminal" influence. In addition, a definition is required as to when "physical or psychological harm" may be said to exist. The current wording could cover any sort of AI-based advertising which influences a person to do something that he or she may later regret.
The particularly strict rules for high-risk AI systems are appropriate as these AI systems pose a higher risk. Limiting them to fields of application in eight particularly risky areas reduces the cost of using AI systems in the remaining areas because many AI systems are used in both very risky and in less risky areas.
The obligation for providers to guarantee that data sets used to develop AI are error free and complete cannot be met. If e.g. an AI system is trained using a company's employee data, these data sets will never be complete because new staff are continually being taken on. With time, therefore, the decisions of the AI system will become better and better.
In addition, clarification is required as to how providers can create transparency so that users are able to interpret the results of their AI systems since the logical conclusions used by AI systems to achieve results are often not even known to the providers. The same applies to the requirement for data sets to be accurate and robust. These rules must be defined, e.g. by way of standards.
Conformity assessments of high-risk AI systems by the providers themselves are inappropriate . Instead, such assessments should always be carried out by independent third parties in order to minimise the danger of superficial assessments.
It will not always be possible for providers of a high-risk AI system to set up a risk-management system allowing the risks of their AI system to be identified comprehensively throughout its entire life-cycle because for this, they depend on information, and especially data, from the user. Furthermore, this is not necessary for high-risk AI systems that do not change once they have been placed on the market. The Regulation should therefore differentiate between high-risk AI systems that no longer change once they are placed on the market and those which continue to learn when they are in use, e.g. through the data which they generate. The latter require stricter regulation than the former. Providers are depending on information from the user in order to meet the obligation to keep technical documentation up to date.
The proposed non-risk-based transparency obligations will increase the public's acceptance of AI. It should, however, be added that natural persons must be informed *in advance* about the interaction with AI systems, not during or after the interaction. The same applies to content created using deep fake systems.
The fact that market surveillance authorities are given unrestricted access to data sets, on the one hand, makes market surveillance easier. However, it is not always possible for providers to meet this obligation as data sets are often only stored for a short duration or not at all, such as in the case of personal data. Clarification is therefore needed on how the obligation to provide access to data can be brought into line with the requirements of the GDPR. Source codes generally constitute essential trade secrets for companies. Authorities should only therefore be given access to source codes as a final resort. The obligation to grant access, including remote access, poses a high security risk.

2 Legal Assessment

2.1 Legislative Competence of the EU

The Regulation is rightly based on a dual legal basis. For most of the provisions, the internal market competence [Art. 114 TFEU] is the correct legal basis. The provisions on using real-time remote biometric identification systems for law enforcement purposes cannot, however, be based on this competence. The data protection competence [Art. 16 TFEU] is the correct legal basis in this regard.

2.2 Subsidiarity

Unproblematic.

2.3 Proportionality with Respect to Member States

The European Artificial Intelligence Board should be upgraded, thereby strengthening the role of the national supervisory authorities in enforcing the Regulation vis à vis the Commission. The Board should not simply be an ancillary body of the Commission but be able to act on its own initiative. In addition, it should be designed analogously to the "independent European Board for Digital Services" in the Digital Services Act proposal (see cep**PolicyBrief** 24/2021). It could then issue recommendations which the national authorities would have to follow or otherwise be required to explain any deviation from the recommendation.

2.4 Compatibility with EU Law in Other Respects

The Commission's powers to amend, by means of delegated acts, the list of AI technologies and concepts that fall under the Regulation, as well as the fields of application of high-risk AI systems, are far-reaching, but remain within the scope of the provisions on delegated acts [Art. 290 TFEU] because they are sufficiently determinate. In particular, the Regulation not only provides that the risk of new fields of application must correspond to that of the existing fields of application, but also provides the criteria to be used for the comparison of risk. In addition, in view of the rapid technical development of AI, there is a risk that amendments to the Regulation would take too long in the ordinary legislative process.

The use of remote biometric identification systems for law enforcement purposes interferes with the right to data protection {Art. 8 CFR]. The Regulation rightly therefore restricts their use, but inadequately protects the right to data protection. Thus, for the persons whose data is captured, it makes little difference whether they are identified in real time or with a time delay of e.g. 24 hours. The Regulation thus falls short. It should focus on the duration and grounds for processing data and prohibit use taking place continuously or over a long period of time and without restriction to a certain occurrence in the past, e.g. an offence recorded on video camera.

The use of AI systems to recognise emotions or biometric categorisation constitutes a serious interference with the right to respect for private life [Art. 7 CFR] and data protection [Art. 8 CFR] and must therefore be subject to stricter requirements than a mere duty of information. Similar to the rules on AI systems for remote biometric identification and the GDPR provisions on the processing of biometric data for the purpose of identification, the Regulation should provide a conclusive list of the purposes for which the use of AI systems designed to recognise emotions or for biometric categorisation is permitted. Such AI systems should also be subject to rigorous examination as to whether they produce accurate results because there is a fundamental question mark over how well e.g. political or sexual orientation can be identified based on external characteristics. Only if this is affirmed should use of AI systems be allowed for the conclusively designated purposes.

The rules on "social scoring" systems must apply not only to authorities but also to private-sector providers because the latter – e.g. social media and cloud service providers – can also collect large amounts of personal data and carry out social scoring on the basis thereof. This should only be permitted if those affected are transparently informed – i.e. not just in the small print – and have given valid consent. In addition, it must be ensured that no-one can circumvent the ban on use by using social scoring results obtained by a third party.

The planned fines of up to € 30 million or 6% of global annual turnover are inappropriately high. Although the threat of penalties which provide effective deterrence to major companies are necessary, the penalties in the AI Regulation exceed the usual rates in other EU legislation. For example, they are 50% higher than those of the GDPR There is no apparent reason for this. In view of the unclear legal terms, which still require judicial definition, there is a danger that the threatened penalties will primarily deter small companies from developing AI systems. This is especially true since AI technology is evolving at a rapid pace and thus new legal issues will continue to arise.